Getech Education

FORTINET

How healthy is your network security?

Secure network architectures need to constantly evolve to keep up with the latest advanced persistent threats. There are two ways to find out if your solution isn't keeping up - wait for a breach to happen or run validation tests.

Designed to help get an in-depth view of the current state of your network using FortiGate to get a clear view of vulnerable areas, a Fortinet Cyber Threat Assessment can help you better understand.

Security risks

Which application vulnerabilities are being used to attack your network, which malware or botnets were detected, what phishing attacks are making it through your defences, which devices are at risk - for security breach probability.

Productivity

Which peer-to-peer, social media, instant messaging and other apps are running - for application visibility control as well as what spam, newsletters or adult content may be bothering your email.

Utilisation

How is your network performing? What is your throughput, session, and bandwidth usage requirements during peak hours - for the network, email system and critical applications.

What are the benefits of running a CTAP?

Quick: 5-7 days of monitoring

Easy: No interruption to your infrastructure

Comprehensive report: Security, Productivity and Performance

No Cost

There are three types of Cyber Threat Assessment available:

CTAP for NGFW

CTAP for NGFW will help you identify security risks and understand your network usage.

VIEW SAMPLE REPORT

CTAP for SD-WAN

CTAP for SD-WAN will help you identify router usage and potential security risks.

VIEW SAMPLE REPORT

CTAP for Email

CTAP for email will help identify gaps in your cloud-based (eg. Office 365) email security.

VIEW SAMPLE REPORT

Contact Getech Education for more information

Getech Education • Solutions Centre • Knightsdale Road • Ipswich IP1 4JQ

www.getech.co.uk/education • team@getecheducation.com • 01473 240470

Copyright © 2021 • All rights reserved • Photographs are for illustration purposes only • E&OE